'338 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
		Reference Manual (March 1997) [SYM_P_0078004-77], Appendix A. SunScreen Firewall. *See* SunScreen EFS Configuration and Management Guide, Release 1.1 (June 1997) [SUN_0000501-856]. SNMP/RMON. *See* my expert report.	value, and label." (170) [SYM_P_0077178] "The host monitor consists of a *host event generator* (HEG) and a *host agent*. The HEG collects and analyzes audit records from the host's operating system. The audit records are scanned for *notable events*, which are transactions that are of interest independent of any other records. These include, among others, failed events, user authentications, changes to the security state of the system, and any network access such as *rlogin* and *rsh*." (169) [SYM_P_0077177] "The LAN monitor is currently a subset of UC Davis' Network Security Monitor [3]. The LAN monitor builds its own 'LAN audit trail'. The LAN monitor observes each and every packet on its segment of the LAN and, from these packets, it is able to construct higher-level objects such as connections (logical circuits), and service requests using the TCP/IP or UDP/IP protocols. In particular, it audits host-to-host connections, services used, and volume of traffic per connection. Similar to the host monitor, the LAN monitor uses several simple analysis techniques to identify significant events. The events include the use of certain services (e.g., *rlogin* and *telnet*) as well as activity by certain classes of hosts (e.g., a PC without a host monitor). The LAN monitor also uses and maintains profiles of expected network behavior. The profiles consist of

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'338 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
			expected data paths (e.g., which systems are expected to establish communication paths to which other systems, and by which service) and service profiles (e.g., what a typical *telnet, mail, or finger* is expected to look like)." (171) [SYM_P_0077179] See '338 claim 5 *See* L. Todd Heberlein., "A Network Security Monitor Final Report" (1995) [SYM_P_0070787-839], 51-53 [SYM_P_0070837-39] (public use). NetRanger. *See* NetRanger User's Guide 1.3.1, WheelGroup Corporation, 1997 [SYM_P_0074948-5282], 4-67 [SYM_P_0075123]. ISS RealSecure. *See* Real Secure 1.1: User Guide and Reference Manual (March 1997) [SYM_P_0078004-77], Appendix A. SunScreen Firewall. *See* SunScreen EFS Configuration and Management Guide, Release 1.1 (June 1997) [SUN_0000501-856]. SNMP/RMON. *See* my expert report.

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'338 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
11	The method of claim 1, further comprising responding based on the determining whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity.	See '203 claim 1 "The proposed architecture for this distributed intrusion-detection system consists of the following components: a host manager (viz. a monitoring process or collection of processes running in background) in each host; a LAN manager for monitoring each LAN in the system; and a central manager which is placed at a single secure location and which receives reports from various host and LAN managers to process these reports, correlate them, and detect intrusions." (1) [SYM_P_0069280] "The director's user interface serves both the intrusion detection and the incident management components of DIDS. It is designed to take advantage of the graphic capabilities of the target platform (a Sun SPARCstation I). The user interface is hierarchical in its presentation of information, allowing the SS0 to display as much, or as little, of the information available from DIDS as he/she wants. In its most compact form, the interface is reduced to a state meter displaying a measure of the security state of the network as evaluated by DIDS. Other options include a control panel for access to system management tools, displays of summary or detailed monitoring of the net, of hosts or of users, and a query capability for the distributed audit data. The user interface is designed to be extensible, so that new functionality can he added without undue effort." (15)	See '203 claim 1 "The architecture also provides for bidirectional communication between the DIDS director and any monitor in the configuration. This communication consists primarily of notable events and anomaly reports from the monitors." (169) [SYM_P_0077177] "We anticipate that a growing set of tools, including incident-handling tools and network-management tools, will be used in conjunction with the intrusion-detection functions of DIDS. This will give the SSO the ability to actively respond to attacks against the system in real-time. Incident-handling tools may consist of possible courses of action to take against an attacker, such as cutting off network access, a directed investigation of a particular user, removal of system access, etc. Network-management tools that are able to perform network mapping would also be useful." (169-70) [SYM_P_0077177-SYM_P_0077178]

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'338 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
		[SYM_P_0069294] "We anticipate that a growing set of tools will be used in conjunction with the intrusion detection functions of DIDS. Among these will include incident handling tools. Depending on the level of expertise of the SSO, these tools could include online explicit instructions, e.g., "who to call" lists, automatic response procedures, etc. In addition to the incident handling tools, the user interface can provide access to standard network administration tools; in particular, we are evaluating the SNMP tools currently available." (15) [SYM_P_0069294]	
12	The method of claim 11, wherein responding comprises transmitting an event record to a network monitor.	See '203 claim 1	See '203 claim 1
13	The method of claim 12, wherein transmitting the event record to a network monitor comprises transmitting the event record to a hierarchically higher network monitor.	See '203 claim 1	See '203 claim 1
14	The method of claim 13, wherein transmitting the event record to a network monitor comprises transmitting the event	See '203 claim 1	See '203 claim 1

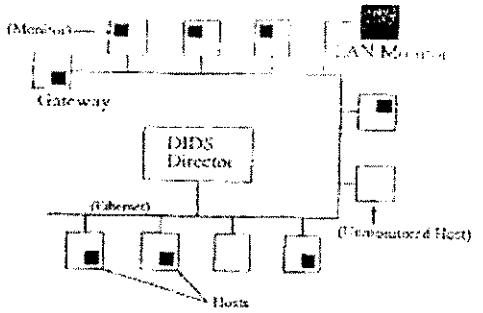
Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'338 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	record to a network monitor that receives event records from multiple network monitors.		
15	The method of claim 14, wherein the monitor that receives event records from multiple network monitors comprises a network monitor that correlates activity in the multiple network monitors based on the received event records.	See '203 claim 2	See '203 claim 2
16	The method of claim 11, wherein responding comprises altering analysis of the network packets.	"The director is responsible for analyzing the events reported by the host and LAN monitors, and therefore will have access to the distributed audit data gathered by the various monitors. The director may then use these records in support of a directed investigation of a particular subject. The director communicates bidirectionally with the host and LAN monitors to facilitate the transfer of data and the processing of queries and responses. It is also able to correlate information obtained from the individual host and LAN monitors. The director also supports the user interface." (12) [SYM_P_0069291]	"The architecture also provides for bidirectional communication management tools as they become useful. This communication consists primarily of notable events and anomaly reports from the monitors. The director can also make request for more detailed information from the distributed monitors via a 'GET' directive, and issue commands to have the distributed monitors modify their monitoring capabilities via a 'SET' directive." (169) [SYM_P_0077177] "Upon request, the LAN monitor is also able to provide a more detailed examination of any connection, including capturing every character crossing the network (i.e., a wire-tap). This capability can be used to support a directed investigation of a particular subject or object." (171) [SYM_P_0077179]

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'338 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
17	The method of claim 11, wherein responding comprises severing a communication channel.	**103:** CIDF. *See* Maureen Stillman, "Revised CIDF Documents" Oct. 6, 1997 [SYM_P_0071236-261], [SYM_P_0071247-48]. AIS. *See* William Hunteman, "Automated Information System—"AIS) Alarm System," Proc. of the 20th National Systems Security Conference (October 1997) [SYM_P_0526260 – SYM_P_0526271], 10 [SYM_P_0526269]. Network Security Probe. *See* P. Rolin, L. Toutain, and S. Gombault, "Network Security Probe," Proc. of the 2nd ACM Conference on Computer and Communications Security, 229-40 (ACM 1994) [SYM_P_0074513 – SYM_P_0074524], 235-37 [SYM_P_0074519-21]. '750 Patent. *See* U.S. Pat. No. 5,825,750 (Thompson) [SYM_P_0076772 – SYM_P_0076781], 5:63-6:6 [SYM_P_0076779]. synkill. *See* Schuba et al., "Analysis of a Denial of Service Attack on TCP," Proc. of the 1997 IEEE Symposium on Security and Privacy, Oakland, CA, 208-23 (May 4-7 1997) [SYM_P_0535408-28], 214-222 [SYM_P_0535419-27].	"We anticipate that a growing set of tools, including incident-handling tools and network-management tools, will be used in conjunction with the intrusion-detection functions of DIDS. This will give the SSO the ability to actively respond to attacks against the system in real-time. Incident-handling tools may consist of possible courses of action to take against an attacker, such as cutting off network access, a directed investigation of a particular user, removal of system access, etc. Network-management tools that are able to perform network mapping would also be useful." (169-70) [SYM_P_0077177-SYM_P_0077178] **103:** CIDF. *See* Maureen Stillman, "Revised CIDF Documents" Oct. 6, 1997 [SYM_P_0071236-261], [SYM_P_0071247-48]. AIS. *See* William Hunteman, "Automated Information System—"AIS) Alarm System," Proc. of the 20th National Systems Security Conference (October 1997) [SYM_P_0526260 – SYM_P_0526271], 10 [SYM_P_0526269]. Network Security Probe. *See* P. Rolin, L. Toutain, and S. Gombault, "Network Security Probe," Proc. of the 2nd ACM Conference on Computer and Communications Security, 229-40

'338 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
			(ACM 1994) [SYM_P_0074513 – SYM_P_0074524], 235-37 [SYM_P_0074519-21]. '750 Patent. *See* U.S. Pat. No. 5,825,750 (Thompson) [SYM_P_0076772 – SYM_P_0076781], 5:63-6:6 [SYM_P_0076779]. synkill. *See* Schuba et al., "Analysis of a Denial of Service Attack on TCP," Proc. of the 1997 IEEE Symposium on Security and Privacy, Oakland, CA, 208-23 (May 4-7 1997) [SYM_P_0535408-28], 214-222 [SYM_P_0535419-27].
18	The method of claim 1, wherein the network packets comprise TCP/IP packets.	"The next layer, called the *thread layer*, accepts as input the time-augmented packets from the packet layer. These packets are then correlated into unidirectional data streams. Each stream consists of the data (with the different layers of protocol headers removed) being transferred from one host to another host by a particular protocol (TCP/IP or UDP/IP), through a unique set (for the particular set of hosts and protocol) of ports. This stream of data, which is called a thread, is mapped into a *thread vector*. All the thread vectors are passed up to the third layer." (10) [SYM_P_0069289]	"The LAN monitor is currently a subset of UC Davis' Network Security Monitor [3]. The LAN monitor builds its own 'LAN audit trail'. The LAN monitor observes each and every packet on its segment of the LAN and, from these packets, it is able to construct higher-level objects such as connections (logical circuits), and service requests using the TCP/IP or UDP/IP protocols. In particular, it audits host-to-host connections, services used, and volume of traffic per connection." (171) [SYM_P_0077179]
19	The method of claim 1, wherein the network entity comprises a gateway, a router, or a proxy	"The generalized distributed environment is heterogeneous, i.e., the network nodes can be hosts or servers from different vendors, or some of them could be LAN managers, like our	"In addition to the current host monitor, which is designed to detect attacks on general purpose multi-user computers, we intend to develop monitors for application specific hosts such as

'338 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	server.	previous work, a network security monitor (NSM), as well." (1) [SYM_P_0069280] **103:** NetRanger: NetRanger User's Guide 1.3.1, WheelGroup Corporation, 1997 [SYM_P_0074948 – SYM_P_0075282]	file servers and gateways. In support of the ongoing development of DIDS we are planning to extend our model to a hierarchical Wide Area Network environment." (174) [SYM_P_0077182]  Fig. 1. DIDS Target Environment [SYM_P_0077184]
21	A method of network surveillance, comprising:	See '338 claim 1	See '338 claim 1
	monitoring network packets handled by a network entity;	See '338 claim 1	See '338 claim 1

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'338 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	building a long-term and multiple short-term statistical profiles of the network packets;	See '338 claim 1 "The abnormality of a connection is based on the probability of that particular connection occurring and the behavior of the connection itself. If a connection from host A to host B by service C is rare, then the abnormality of that connection is high. Furthermore, if the profile of that connection compared to a typical connection by the same type of service is unusual (e.g., the number of packets or bytes is unusually high for a *mail* connection), the abnormality of that connection is high." (11) [SYM_P_0069290] "The NSM (adaptively) develops profiles of usage of network resources and then compares current usage patterns with the historical profile to determine possible security violations. The goal of our proposed research is to extend our network intrusion-detection concept from the LAN environment to arbitrarily wider areas with the network topology being arbitrary as well." (11) [SYM_P_0069290]	See '338 claim 1
	comparing one of the multiple short-term statistical profiles with the long-term statistical profile; and	See '338 claim 1	See '338 claim 1

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'338 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	determining whether the difference between the one of the multiple short-term statistical profiles and the long-term statistical profile indicates suspicious network activity.	See '338 claim 1	See '338 claim 1
24	A computer program product, disposed on a computer readable medium, the product including instructions for causing a processor to:	See '338 claim 1	See '338 claim 1
	receive network packets handled by a network entity;	See '338 claim 1	See '338 claim 1
	build at least one long-term and at least one short-term statistical profile from at least one measure of the network packets,	See '338 claim 1	See '338 claim 1
	the measure monitoring data transfers, errors, or network connections;	See '338 claim 1	See '338 claim 1
	compare at least one short-term and at least one long-term statistical profile; and	See '338 claim 1	See '338 claim 1
	determine whether the difference between the short-	See '338 claim 1	See '338 claim 1

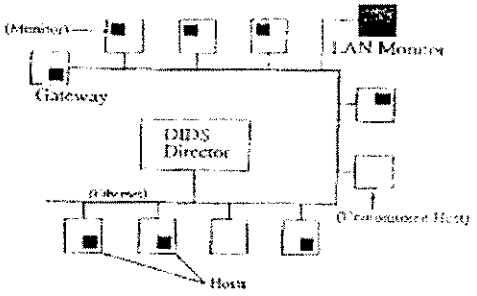
Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'338 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	term statistical profile and the long-term statistical profile indicates suspicious network activity.		
25	A method of network surveillance, comprising:	See '338 claim 1	See '338 claim 1
	receiving packets at a virtual private network entity; and	**103:** SunScreen Firewall. *See* SunScreen EFS Configuration and Management Guide, Release 1.1 (June 1997) [SUN_0000501-856], 2-5 to 2-10 [SUN_000549-54]. NetRanger. *See* NetRanger User's Guide 1.3.1, WheelGroup Corporation, 1997 [SYM_P_0074948-5282], 1-13 to 1-14 [SYM_P_0074986-87], B-10 to B-17 [SYM_P_0075204-11]. U.S. Patent No. 5,825,891 (Levesque) Key Management for Network Communication 10/29/1997 [SYM_P_0069852-SYM_P_0069866]	**103:** SunScreen Firewall. *See* SunScreen EFS Configuration and Management Guide, Release 1.1 (June 1997) [SUN_0000501-856], 2-5 to 2-10 [SUN_000549-54]. NetRanger. *See* NetRanger User's Guide 1.3.1, WheelGroup Corporation, 1997 [SYM_P_0074948-5282], 1-13 to 1-14 [SYM_P_0074986-87], B-10 to B-17 [SYM_P_0075204-11]. U.S. Patent No. 5,825,891 (Levesque) Key Management for Network Communication 10/29/1997 [SYM_P_0069852-SYM_P_0069866]
	building at least one long-term and at least one short-term statistical profile based on the received packets, and	See '338 claim 1	See '338 claim 1
	comparing at least one long-	See '338 claim 1	See '338 claim 1

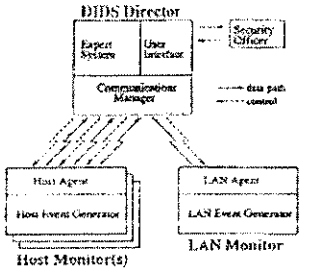
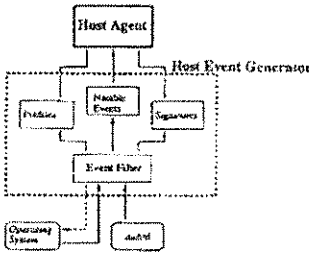
Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'338 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	term statistical profile with at least one short-term statistical profile to determine whether the packets indicate suspicious network activity.		

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
1	A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:	"Previous work on intrusion-detection systems were performed on stand-alone hosts and on a broadcast local area network (LAN) environment. The focus of our present research is to extend our network intrusion-detection concept from the LAN environment to arbitrarily wider areas with the network topology being arbitrary as well. The generalized distributed environment is heterogeneous, i.e., the network nodes can be hosts or servers from different vendors, or some of them could be LAN managers, like our previous work, a network security monitor (NSM), as well. The proposed architecture for this distributed intrusion-detection system consists of the following components: a host manager (viz. a monitoring process or collection of processes running in background) in each host; a LAN manager for monitoring each LAN in the system; and a central manager which is placed at a single secure location and which receives reports from various host and LAN managers to process these reports, correlate them, and detect intrusions." (1) [SYM_P_0069280]	"We are designing and implementing a prototype Distributed Intrusion Detection System (DIDS) that combines distributed monitoring and data reduction (through individual host and LAN monitors) with centralized data analysis (through the DIDS director) to monitor a heterogeneous network of computers. This approach is unique among current IDS's." (167) [SYM_P_0077175]  Fig. 1. DIDS Target Environment [SYM_P_0077184]

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
			 Fig. 2. Communications Architecture  Fig. 3. Host Monitor Structure [SYM_P_0077184]

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	deploying a plurality of network monitors in the enterprise network;	"DIDS is a proposed distributed intrusion detection system that is intended to enhance the effectiveness and efficiency of the SSO in monitoring a network of computers. DIDS is designed to discover attacks on, and misuse of, individual hosts as well as the network which connects them. It looks for attempts to subvert or avoid authentication as well as other methods of gaining unauthorized access to, or privileges on, the monitored computers. It also attempts to detect masqueraders and insiders committing a variety of offenses, e.g., espionage or data alteration. The system is based on both known and hypothesized abuses. It is designed to operate in near real time, providing for both general surveillance and focused investigation. The analysis portion of the system utilizes an inference network and incorporates learning algorithms so that it can deal with new forms of attacks and abuse as they develop. The inference network is also supported by an explanation facility which lets the operator examine the system's chain of reasoning. DIDS incorporates various ideas from a number of its predecessors." (12) [SYM_P_0069291] "In DIDS, the monitoring and analysis functions are distributed among several components. These components include a *DIDS director*, a collection of *host monitors*, and at least one *LAN monitor*. The host and LAN monitors are primarily responsible for detecting single events and known attack signatures which have a high probability of being relevant to the security of a system; so	"This paper describes a prototype Distributed Intrusion Detection System (DIDS) which generalizes the target environment in order to monitor multiple hosts connected via a network as well as the network itself. The DIDS components include the DIDS director, a single host monitor per host, and a single LAN monitor for each LAN segment of the monitored network. The information gathered by these distributed components is transported to, and analyzed at, a central location (viz. an expert system, which is a sub-component of the director), thus providing the capability to aggregate information from different sources. We can cope with any audit trail format as long as the events of interest are provided." (168) [SYM_P_0077176]

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
		they must constantly monitor their respective domains." (12) [SYM_P_0069291]	
	detecting, by the network monitors, suspicious network activity	"We believe that DIDS will be able to detect the same kind of single host intrusions that are flagged by other intrusion detection systems, such as IDES [6], Wisdom & Sense [15], and MIDAS [10]. DIDS should also be able to (1) detect attacks on the network itself, (2) detect attacks involving multiple hosts, (3) track tagged objects, including users and sensitive files, as they move around the network, (4) detect, via erroneous or misleading reports, situations where a host might be taken over by an attacker, and (5) monitor the activity of any networked system that doesn't have a host monitor, yet generates LAN activity, such as a PC." (15) [SYM_P_0069294] "The DIDS LAN monitor is built on the same foundation as UC Davis' Network Security Monitor [5]. Since there is no native LAN audit trail, the LAN monitor is responsible for building its own. The LAN monitor sees every packet on its segment of the LAN. From these packets, the LAN monitor is able to construct higher level objects such as connections (logical circuits), and service requests. In particular, it audits host-to-host connections, services used, and volume of traffic. Like the host based monitor, the LAN monitor uses several levels of analysis to catch the most significant events, for example, sudden changes in network load,	"The detection of certain attacks against a networked system of computers requires information from multiple sources. A simple example of such an attack is the so-called *doorknob* attack. In a doorknob attack the intruder's goal is to discover, and gain access to, insufficiently-protected hosts on a system. The intruder generally tries a few common account and password combinations on each of a number of computers. These simple attacks can be remarkably successful [4]. As a case in point, UC Davis' NSM recently observed an attacker of this type gaining super-user access to an external computer which did not require a password for the super-user account. In this case, the intruder used *telnet* to make the connection from a university computer system, and then repeatedly tried to gain access to several different computers at the external site. In cases like these, the intruder tries only a few logins on each machine (usually with different account names), which means that an IDS on each host may not flag the attack. Even if the behavior is recognized as an attack on the individual host, current IDS's are generally unable to correlate reports from multiple hosts; thus they cannot recognize the *doorknob* attack as such. Because DIDS aggregates and correlates data from multiple hosts and the network, it is in a position to recognize the doorknob attack by detecting the pattern of repeated failed logins even

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
		the use of security-related services, and network activities such as *rlogin*. As with the host monitor, the LAN monitor retains the audit data for analysis by the director. It also uses and maintains profiles of network behavior, which are updated periodically. Like the host monitor, the LAN monitor provides an agent for communications with the director. In addition to handling queries of the audit data from the director, this agent gives the director access to a number of network management tools, which are analogous to the host." (13) [SYM_P_0069292] "[5] L.T. Heberlein, G. Dias, K. Kevitt, B. Mukherjee, J Wood, and D. Wolber, "A Network Security Monitor," Proc. 1990 Symposium on Research in Security and Privacy, pp. 296-304, Oakland, CA, May 1990." (15) [SYM_P_0069294]	though there may be too few on a single host to alert that host's monitor. "In another incident, our NSM recently observed an intruder gaining access to a computer using a guest account which did not require a password. Once the attacker had access to the system, he exhibited behavior which would have alerted most existing IDS's (e.g., changing passwords and failed events). In an incident such as this, DIDS would not only report the attack, but may also be able to identify the source of the attack. That is, while most IDS's would report the occurrence of an incident involving user "guest" on the target machine, DIDS would also report that user "guest" was really, for example, user "smith" on the source machine, assuming that the source machine was in the monitored domain. It may also be possible to go even further back and identify all of the different user accounts in the "chain" to find the initial launching point of the attack. "Another possible scenario is what we call *network browsing*. This occurs when a (network) user is looking through a number of files on several different computers within a short period of time. The browsing activity level on any single host may not be sufficiently high enough to raise any alarm by itself. However, the network-wide, aggregated browsing activity level may be high enough to raise suspicion on this user. Network browsing can be

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
			detected as follows. Each host monitor will report that a particular user is browsing on that system, even if the corresponding degree of browsing is small. The expert system can then aggregate such information from multiple hosts to determine that all of the browsing activity corresponds to the same network user. This scenario presents a key challenge for DIDS: the tradeoff between sending all audit records to the director versus missing attacks because thresholds on each host are not exceeded. "In addition to the specific scenarios outlined above, there are a number of general ways that an intruder can use the connectivity of the network to hide his trail and to enhance his effectiveness. Some of the attack configurations which have been hypothesized include *chain* and *parallel* attacks [2]. DIDS combats these inherent vulnerabilities of the network by using the very same connectivity to help track and detect the intruder. Note that DIDS should be at least as effective as host-based IDS's (if we implement all of their functionality in the DIDS host monitor), and at least as effective as the stand-alone NSM." (168-69) [SYM_P_0077176- SYM_P_0077177]
	based on analysis of network traffic data selected from the following categories: {network packet	"The LAN monitor sees every packet on its segment of the LAN. From these packets, the LAN monitor is able to construct higher level objects such as connections (logical circuits), and service requests. In particular, it audits host-to-host connections, services	"Like the host monitor, the LAN monitor consists of a *LAN event generator* (LEG) and a *LAN agent*. The LEG is currently a subset of UC Davis' NSM [3]. Its main responsibility is to observe all of the traffic on its segment of the LAN to monitor host-to-host

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet};	used, and volume of traffic." (13) [SYM_P_0069292] "The NSM models the network and hosts being monitored in the hierarchically-structured Interconnected Computing Environment Model (ICEM). The ICEM is composed of six layers, the lowest being the bit streams on the network, and the highest being a representation for the suite of the entire networked system. The bottom-most, or first, layer is the packet layer. This layer accepts as input a bit stream from a broadcast local area network, viz. an Ethernet. The bit stream is divided up into complete Ethernet packets, and a time stamp is attached to the packet. This *time-augmented packet* is then passed up to the second layer. The next layer, called the *thread layer*, accepts as input the time-augmented packets from the packet layer. These packets are then correlated into unidirectional data streams. Each stream consists of the data (with the different layers of protocol headers removed) being transferred from one host to another host by a particular protocol (TCP/IP or UDP/IP), through a unique set (for the particular set of hosts and protocol) of ports. This stream of data, which is called a thread, is mapped into a *thread vector*. All the thread vectors are passed up to the third layer. The *connection layer*, which is the third layer, accepts as input the	connections, services used, and volume of traffic. The LAN monitor reports on such network activity as *rlogin* and *telnet* connections, the use of security-related services, and changes in network traffic patterns." (169) [SYM_P_0077177] "An event reported by a LAN monitor is called a network audit record (nar). The record syntax is: nar(Monitor-ID, Source_Host, Dest_Host, Time, Service, Domain, Status)." (172) [SYM_P_0077180] "The LAN monitor is currently a subset of UC Davis' Network Security Monitor [3]. The LAN monitor builds its own 'LAN audit trail'. The LAN monitor observes each and every packet on its segment of the LAN and, from these packets, it is able to construct higher-level objects such as connections (logical circuits), and service requests using the TCP/IP or UDP/IP protocols. In particular, it audits host-to-host connections, services used, and volume of traffic per connection." (171) [SYM_P_0077179]

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
		thread vectors generated by the thread layer. Each thread vector is paired, if possible, to another thread vector to represent a bidirectional stream of data (i.e., a host-to-host connection). These pairs of thread vectors are represented by a connection vector generated by the combination of the individual thread vectors. Each connection vector will be analyzed, and a reduced representation, a *reduced connection vector*, is passed up to the fourth layer. Layer 4 is the *host layer* which accepts as input the reduced connection vectors generated by the connection layer. The connection vectors are used to build host vectors. Each host vector represents the network activities of a single host. These host vectors are passed up to the fifth layer. The *connected network* layer is the next layer in the ICEM hierarchy. It accepts as input the host vectors generated by the host layer. The host vectors are transformed into a graph C by treating the Data_path_tuples of the host vectors as an adjacency list. If G(host1,host2,serv1) is not empty, then there is a connection, or path, from host1 to host2 by service serv1. The value for location G(host1,host2,serv1) is non empty if the host vector for host1 has (host2,serv1) in it's Data_path_tuples. This layer can build the connected sub-graphs of G, called a connected *network vector*, and compare these sub-graphs against historical	

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
		connected sub-graphs. This layer can also accept questions from the user about the graph. For example, the user may ask if there is some path between two hosts through any number of intermediate hosts — by a specific service. This set of connected network vectors is passed up to the sixth and final layer. The top most layer, called the *system layer*, accepts as input the set of connected network vectors from the connected network layer. The set of connected network vectors are used to build a single *system vector* representing the behavior of the entire system." (10) [SYM_P_0069289] "Our previous work concentrated on the development of an intrusion-detection model and a prototype implementation of a network security monitor (NSM) for a broadcast local area network environment [5]. The NSM (adaptively) develops profiles of usage of network resources and then compares current usage patterns with the historical profile to determine possible security violations. The goal of our proposed research is to extend our network intrusion-detection concept from the LAN environment to arbitrarily wider areas with the network topology being arbitrary as well." (11) [SYM_P_0069290] "The DIDS LAN monitor is built on the same foundation as UC Davis' Network Security Monitor [5]. Since there is no native	

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
		LAN audit trail, the LAN monitor is responsible for building its own. The LAN monitor sees every packet on its segment of the LAN. From these packets, the LAN monitor is able to construct higher level objects such as connections (logical circuits), and service requests. In particular, it audits host-to-host connections, services used, and volume of traffic. Like the host based monitor, the LAN monitor uses several levels of analysis to catch the most significant events, for example, sudden changes in network load, the use of security-related services, and network activities such as *rlogin*. As with the host monitor, the LAN monitor retains the audit data for analysis by the director. It also uses and maintains profiles of network behavior, which are updated periodically. Like the host monitor, the LAN monitor provides an agent for communications with the director. In addition to handling queries of the audit data from the director, this agent gives the director access to a number of network management tools, which are analogous to the host." (13) [SYM_P_0069292] "The *Network Security Monitor* (NSM) is different from the intrusion detection systems discussed in Section 2 in that it does not analyze audit trails to detect intrusive behavior. The NSM, as the name implies, analyzes the traffic on a broadcast local area network to detect intrusive behavior. The reasons for this departure from the standard intrusion detection methods are outlined as follows.	

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
		"First, although most IDSs are designed with the goal of supporting a number of different operating system platforms, all present audit-trail-based IDSs have only been used on a single operating system at any one time. These systems are usually designed to transform an audit log into a proprietary format used by the IDS [6, 10, 11]. In theory, audit logs from different operating systems need only to be transformed into this proprietary form for the IDS to perform its analysis. However, no results of an IDS successfully supporting multiple operating systems have been reported. "On the other hand, standard network protocols exist (e.g., TCP/IP and UDP/IP) which most major operating systems support and use. By using these network standards, the NSM can monitor a heterogeneous set of hosts and operating systems simultaneously. "Second, audit trails are often not available in a timely fashion. Some IDSs are designed to perform their analysis on a separate host, so the audit logs must be transferred from the source host to the second host monitor [11]. Furthermore, the operating system can often delay the writing of audit logs by several minutes [15]. The broadcast nature of local area networks, however, gives the NSM instant access to all data as soon as thus data is transmitted on the network. It is then possible to immediately start the attack	

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
		detection process. "Third, the audit trails are often vulnerable. In some past incidents, the intruders have turned off audit daemons or modified the audit trail. This action can either prevent the detection of the intrusion, or it can remove the capability to perform accountability (who turned off the audit daemons'?) and damage control (what was seen, modified, or destroyed?) The NSM, on the other hand, passively listens to the network, and is therefore logically protected from subversion. Since the NSM is invisible to the intruder, it cannot be turned off (assuming it is physically secured), and the data it collects cannot be modified. "Fourth, the collection of audit trails degrades the performance of a machine being monitored. Unless audit trails are being used for accounting purposes, system administrators often turn off auditing. If analysis of these audit logs is also to be performed on the host, added degradation will occur, if the audit logs are transferred across a network or communication channel to a separate host for analysis, the loss of network bandwidth, as well as the loss of timeliness of the data will occur. In many environments, the degradation of monitored hosts or the loss of network bandwidth may discourage administrators from using such an IDS. The alternative, viz. the NSM architecture, does not degrade the performance of the hosts being monitored. The	

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
		monitored hosts are not aware of the NSM, so the effectiveness of the NSM is not dependent on the system administrator's configuration of the monitored hosts. "And, finally, many of the more seriously documented cases of computer intrusions have utilized a network at some point during the intrusion, i.e., the intruder was physically separated from the target. With the continued proliferation of networks and interconnectivity, the use of networks in attacks will only increase. Furthermore, the network itself, being an important component of a computing environment, can be the object of an attack. The NSM can take advantage of the increase of network usage to protect the hosts attached to the networks. It can monitor attacks launched against the network itself, an attack that host based audit trail analyzers would probably miss." (9-10) [SYM_P_0069288- SYM_P_0069289]	

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
		Table I CONNECTION VECTOR; Table II HOST VECTOR (below) [SYM_P_0069296]	

Table I CONNECTION VECTOR

Component	Description
Connection ID	Unique integer used to reference this particular connection.
Initiator_address	The internet address of the host which initiated the connection.
Receiver_address	The internet address of the host to which the connection was made.
Service	An integer used to identify the particular service (i.e., telnet or mail) used for this connection.
Start_time	The time stamp on the first packet received for this connection.
Delta_time	The difference between the time stamp of the most recent packet for this connection and the Start_time.
Connection_state	The state of the connection. States [illegible] NEW_CONNECTION, CONNECTION_IN_PROGRESS, and CONNECTION_CLOSED.
Security_state	The current evaluation of the security state of this connection.
Initiator_pkts	The number of packets the host which initiated the connection has placed on the network.
Initiator_bytes	The number of bytes, excluding protocol headers, contained in the packets.
Receiver_pkts	The number of packets the host which received the connection has placed on the network.
Receiver_bytes	The number of bytes, excluding protocol headers, contained in the packets.
Transmission	The [illegible] of the Initiator_X and the Receiver_X vectors. The value is the number of strings [illegible] being looked for in the data.
Initiator_X	A vector representing the number of strings matched in Initiator Items.
Receiver_X	A vector representing the number of strings matched in Receiver Items.

Table II HOST VECTOR

Component	Description
Host ID	Unique integer used to reference this particular host.
Host address	The internet address of this host.
Host state	The state of the host. States include ACTIVE, NOT_ACTIVE.
Security_state	The current evaluation of the security of this particular host.
Data_path_number	The number of data paths the currently associated to this host. It may be considered the number of data from a node in a graph.
Data_path_tuples	A list of four-tuple representing a data path from/to the host. The path consists of Other_host_address, Service, ID, Initiator_flag, and Security_state of the data path.

[SYM_P_0069296]

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	generating, by the monitors, reports of said suspicious activity; and	"The generalized distributed environment is heterogeneous, i.e., the network nodes can be hosts or servers from different vendors, or some of them could be LAN monitors, like our NSM, as well. The proposed architecture for this distributed intrusion-detection system consists of three major components. First, there is a host monitor on each host that is required to be monitored by the system. This monitor is a collection of processes running in background in the host. Second, each LAN segment has a LAN monitor, which operates just like a host monitor except that it analyzes LAN traffic. Finally, there is the DIDS director which is placed at a single secure location. The director receives reports from various host and LAN monitors, and by processing and correlating these reports, it is expected to detect intrusions." (11-12) [SYM_P_0069290- SYM_P_0069291] "4.5. LAN Monitor The DIDS LAN monitor is built on the same foundation as UC Davis' Network Security Monitor [5]. Since there is no native LAN audit trail, the LAN monitor is responsible for building its own. The LAN monitor sees every packet on its segment of the LAN. From these packets, the LAN monitor is able to construct higher level objects such as connections (logical circuits), and service requests. In particular, it audits host-to-host connections,	"An event reported by a LAN monitor is called a network audit record (nar). The record syntax is: nar(Monitor-ID, Source_Host, Dest_Host, Time, Service, Domain, Status)." (172) [SYM_P_0077180] "An event reported by a host monitor is called a host audit record (har). The record syntax is: har(Monitor-ID, Host-ID, Audit-UID, Real-UID, Effective-UID, Time, Domain, Action, Transaction, Object, Parent Process, PID, Return Value, Error Code)." (171) [SYM_P_0077179]

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
		services used, and volume of traffic. Like the host based monitor, the LAN monitor uses several levels of analysis to catch the most significant events, for example, sudden changes in network load, the use of security-related services, and network activities such as *rlogin*. As with the host monitor, the LAN monitor retains the audit data for analysis by the director. It also uses and maintains profiles of network behavior, which are updated periodically. Like the host monitor, the LAN monitor provides an agent for communications with the director. In addition to handling queries of the audit data from the director, this agent gives the director access to a number of network management tools, which are analogous to the host operating system services provided by the host monitor." (13) [SYM_P_0069292] "The host monitor incorporates three levels of analysis performed on the HARs. At the lowest level, the host monitor scans each HAR for *notable events*. Notable events are transactions that may be of interest independent of their context (i.e., independent of previous HARs). Examples of notable events include any type of network activity, failed file accesses, accessing system files, and changing a file's access control. At the next higher level, the host monitor looks for *sequences* of events which may be interesting. Known attack signatures or patterns of abuse are examples of sequences which would be of interest. We are developing a general purpose approximate pattern matcher which will be used	

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
		for this purpose. Finally, the host monitor looks for anomalous behavior by tracking user behavior patterns, such as number of programs executed, number of files accessed, etc. As noted above, there are performance trade offs to be considered when deciding how much analysis should be done at the host monitor. When a host monitor notes an interesting event or pattern, it alerts the director and forwards the relevant information. The lists of notable events, the templates for pattern matching, and the metrics for anomaly detection are maintained separately to allow for easy modification." (13) [SYM_P_0069292]	
	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	"The generalized distributed environment is heterogeneous, i.e., the network nodes can be hosts or servers from different vendors, or some of them could be LAN monitors, like our NSM, as well. The proposed architecture for this distributed intrusion-detection system consists of three major components. First, there is a host monitor on each host that is required to be monitored by the system. This monitor is a collection of processes running in background in the host. Second, each LAN segment has a LAN monitor, which operates just like a host monitor except that it analyzes LAN traffic. Finally, there is the DIDS director which is placed at a single secure location. The director receives reports from various host and LAN monitors, and by processing and correlating these reports, it is expected to detect intrusions." (11-12) [SYM_P_0069290- SYM_P_0069291]	"We are designing and implementing a prototype Distributed Intrusion Detection System (DIDS) that combines distributed monitoring and data reduction (through individual host and LAN monitors) with centralized data analysis (through the DIDS director) to monitor a heterogeneous network of computers. This approach is unique among current IDS's." (167) [SYM_P_0077175] "The information gathered by these distributed components is transported to, and analyzed at, a central location (viz. an expert system, which is a sub-component of the director), thus providing the capability to aggregate information from different sources. We can cope with any audit trail format as long as the events of interest are provided." (168) [SYM_P_0077176]

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
		"In addition to refining these approaches, DIDS provides a new dimension to intrusion detection by facilitating the correlation and analysis of data from multiple sources. The target environment will consist of a single physical segment of a local area network with approximately 10 hosts running at least 2 different C2-level secure operating systems." (12) [SYM_P_0069291] "The director is responsible for analyzing the events reported by the host and LAN monitors, and therefore will have access to the distributed audit data gathered by the various monitors. The director may then use these records in support of a directed investigation of a particular subject. The director communicates bidirectionally with the host and LAN monitors to facilitate the transfer of data and the processing of queries and responses. It is also able to correlate information obtained from the individual host and LAN monitors. The director also supports the user interface." (12) [SYM_P_0069291] "The division of labor between the central and distributed components of DIDS is straight-forward. Correlation of the data from multiple sources must be done at the director. Platform specific transformations of information should clearly be done on the individually monitored hosts. However, there is a trade-off between doing some of the analysis on the distributed monitors	"The detection of certain attacks against a networked system of computers requires information from multiple sources. A simple example of such an attack is the so-called *doorknob* attack. In a doorknob attack the intruder's goal is to discover, and gain access to, insufficiently-protected hosts on a system. The intruder generally tries a few common account and password combinations on each of a number of computers. These simple attacks can be remarkably successful [4]. As a case in point, UC Davis' NSM recently observed an attacker of this type gaining super-user access to an external computer which did not require a password for the super-user account. In this case, the intruder used *telnet* to make the connection from a university computer system, and then repeatedly tried to gain access to several different computers at the external site. In cases like these, the intruder tries only a few logins on each machine (usually with different account names), which means that an IDS on each host may not flag the attack. Even if the behavior is recognized as an attack on the individual host, current IDS's are generally unable to correlate reports from multiple hosts; thus they cannot recognize the *doorknob* attack as such. Because DIDS aggregates and correlates data from multiple hosts and the network, it is in a position to recognize the doorknob attack by detecting the pattern of repeated failed logins even though there may be too few on a single host to alert that host's monitor.

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
		and doing it all on the director. If more work is done on the distributed monitors, it will reduce the chance that the processing capability of the director will be a bottleneck, and it will also reduce the amount of data that must be sent across the network. On the other hand, increasing the amount of analysis that is done on the distributed monitors will obviously hinder the performance of the individual hosts." (12) [SYM_P_0069291] "The director is responsible for analyzing the events reported by the host and LAN monitors, and therefore will have access to the distributed audit data gathered by the various monitors. The director may then use these records in support of a directed investigation of a particular subject. The director communicates bidirectionally with the host and LAN monitors to facilitate the transfer of data and the processing of queries and responses. It is also able to correlate information obtained from the individual host and LAN monitors. The director also supports the user interface." (12) [SYM_P_0069291] "This paper presented an architecture for a Distributed Intrusion Detection System (DIDS). The target environment for DIDS is a heterogeneous network of computers that may consist of different hosts, servers, etc. The DIDS architecture consists of a collection of host monitors, each of which monitors a single host Computer; one or more LAN monitors, each of which monitors traffic on its	In another incident, our NSM recently observed an intruder gaining access to a computer using a guest account which did not require a password. Once the attacker had access to the system, he exhibited behavior which would have alerted most existing IDS's (e.g., changing passwords and failed events). In an incident such as this, DIDS would not only report the attack, but may also be able to identify the source of the attack. That is, while most IDS's would report the occurrence of an incident involving user "guest" on the target machine, DIDS would also report that user "guest" was really, for example, user "smith" on the source machine, assuming that the source machine was in the monitored domain. It may also be possible to go even further back and identify all of the different user accounts in the "chain" to find the initial launching point of the attack. Another possible scenario is what we call *network browsing*. This occurs when a (network) user is looking through a number of files on several different computers within a short period of time. The browsing activity level on any single host may not be sufficiently high enough to raise any alarm by itself. However, the network-wide, aggregated browsing activity level may be high enough to raise suspicion on this user. Network browsing can be detected as follows. Each host monitor will report that a particular user is browsing on that system, even if the corresponding degree of browsing is small. The expert system can then aggregate such

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
		corresponding LAN segment; and the DIDS director, which receives reports from the various monitors, correlates the data, and makes inferences regarding the security state of the system." (15) [SYM_P_0069294]	information from multiple hosts to determine that all of the browsing activity corresponds to the same network user. This scenario presents a key challenge for DIDS: the tradeoff between sending all audit records to the director versus missing attacks because thresholds on each host are not exceeded. In addition to the specific scenarios outlined above, there are a number of general ways that an intruder can use the connectivity of the network to hide his trail and to enhance his effectiveness. Some of the attack configurations which have been hypothesized include *chain* and *parallel* attacks [2]. DIDS combats these inherent vulnerabilities of the network by using the very same connectivity to help track and detect the intruder. Note that DIDS should be at least as effective as host-based IDS's (if we implement all of their functionality in the DIDS host monitor), and at least as effective as the stand-alone NSM." (168-69) [SYM_P_0077176- SYM_P_0077177] "The DIDS architecture combines distributed monitoring and data reduction with centralized data analysis." (169) [SYM_P_0077177] "Reports are sent independently and asynchronously from the host and LAN monitors to the DIDS director through a communications infrastructure (Fig. 2). High level communication

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
			protocols between the components are based on the ISO Common Management Information Protocol (CMIP) recommendations, allowing for future inclusion of CMIP management tools as they become useful. The architecture also provides for bidirectional communication between the DIDS director and any monitor in the configuration. This communication consists primarily of notable events and anomaly reports from the monitors. The director can also make requests for more detailed information from the distributed monitors via a 'GET' directive, and issue commands to have the distributed monitors modify their monitoring capabilities via a 'SET' directive." (169) [SYM_P_0077177] "The expert system is responsible for evaluating and reporting on the security state of the monitored system. It receives the reports from the host and the LAN monitors, and, based on these reports, it makes inferences about the security of each individual host, as well as the system as a whole." (169) [SYM_P_0077177] "Correlating data from several independent sources, including the network itself, can aid in recognizing this type of behavior and tracking an intruder to their source." (170) [SYM_P_0077178] "The expert system uses rules derived from the hierarchical Intrusion Detection Model (IDM). The IDM describes the data abstractions used in inferring an attack on a network of computers.

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
			That is, it describes the transformation from the distributed raw audit data to high level hypotheses about intrusions and about the overall security of the monitored environment. In abstracting and correlating data from the distributed sources, the model builds a virtual machine which consists of all the connected hosts as well as the network itself. This unified view of the distributed system simplifies the recognition of intrusive behavior which spans individual hosts. The model is also applicable to]he trivial network of a single computer." (172) [SYM_P_0077180] "Events in context are combined to create threats." (172) [SYM_P_0077180] "At the highest level, the model produces a numeric value between one and 100 which represents the overall *security state* of the network. The higher the number the less secure the network. This value is a function of all the threats for all the subjects on the system. Here again we treat the collection of hosts as a single distributed system. Although representing the security level of the system as a single value seems to imply some loss of information, it provides a quick reference point for the SSO. In fact, in the current implementation, no information is lost since the expert system maintains all the evidence used in calculating the security state in its internal database, and the SSO has access to that database." (173) [SYM_P_0077181] "The expert system shell consists of approximately a hundred

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
			lines of Prolog source code. The shell is responsible for reading new facts reported by the distributed monitors, attempting to apply the rules to the facts and hypotheses in the Prolog database, reporting suspected intrusions, and maintaining the various dynamic values associated with the rules and hypotheses." (173) [SYM_P_0077181] "In addition to the consideration of external temporal context, the expert system uses time windows to correlate events occurring in temporal proximity. This notion of temporal proximity implements the heuristic that a call to the UNIX *who* command followed closely by a *login* or *logout* is more likely to be related to an intrusion than either of those events occurring alone. Spatial context implies the relative importance of the source of events. That is, events related to a particular user, or events from a particular host, may be more likely to represent an intrusion than similar events from a different source. For instance, a user moving from a low-security machine to a high-security machine may be of greater concern than a user moving in the opposite direction. The model also allows for the correlation of multiple events from the same user or source. In both of these cases, the multiple events are more noteworthy when they have a common element than when they do not." (172) [SYM_P_0077180]
2	The method of claim 1,	"The generalized distributed environment is heterogeneous, i.e.,	"We are designing and implementing a prototype Distributed

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	wherein integrating comprises correlating intrusion reports reflecting underlying commonalities.	the network nodes can be hosts or servers from different vendors, or some of them could be LAN monitors, like our NSM, as well. The proposed architecture for this distributed intrusion-detection system consists of three major components. First, there is a host monitor on each host that is required to be monitored by the system. This monitor is a collection of processes running in background in the host. Second, each LAN segment has a LAN monitor, which operates just like a host monitor except that it analyzes LAN traffic. Finally, there is the DIDS director which is placed at a single secure location. The director receives reports from various host and LAN monitors, and by processing and correlating these reports, it is expected to detect intrusions." (11-12) [SYM_P_0069290- SYM_P_0069291] "In addition to refining these approaches, DIDS provides a new dimension to intrusion detection by facilitating the correlation and analysis of data from multiple sources. The target environment will consist of a single physical segment of a local area network with approximately 10 hosts running at least 2 different C2-level secure operating systems." (12) [SYM_P_0069291] "The director is responsible for analyzing the events reported by the host and LAN monitors, and therefore will have access to the distributed audit data gathered by the various monitors. The director may then use these records in support of a directed	Intrusion Detection System (DIDS) that combines distributed monitoring and data reduction (through individual host and LAN monitors) with centralized data analysis (through the DIDS director) to monitor a heterogeneous network of computers. This approach is unique among current IDS's." (167) [SYM_P_0077175] "The information gathered by these distributed components is transported to, and analyzed at, a central location (viz. an expert system, which is a sub-component of the director), thus providing the capability to aggregate information from different sources. We can cope with any audit trail format as long as the events of interest are provided." (168) [SYM_P_0077176] "The detection of certain attacks against a networked system of computers requires information from multiple sources. A simple example of such an attack is the so-called *doorknob* attack. In a doorknob attack the intruder's goal is to discover, and gain access to, insufficiently-protected hosts on a system. The intruder generally tries a few common account and password combinations on each of a number of computers. These simple attacks can be remarkably successful [4]. As a case in point, UC Davis' NSM recently observed an attacker of this type gaining super-user access to an external computer which did not require a password for the super-user account. In this case, the intruder used *telnet* to

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
		investigation of a particular subject. The director communicates bidirectionally with the host and LAN monitors to facilitate the transfer of data and the processing of queries and responses. It is also able to correlate information obtained from the individual host and LAN monitors. The director also supports the user interface." (12) [SYM_P_0069291] "The division of labor between the central and distributed components of DIDS is straight-forward. Correlation of the data from multiple sources must be done at the director. Platform specific transformations of information should clearly be done on the individually monitored hosts. However, there is a trade-off between doing some of the analysis on the distributed monitors and doing it all on the director. If more work is done on the distributed monitors, it will reduce the chance that the processing capability of the director will be a bottleneck, and it will also reduce the amount of data that must be sent across the network. On the other hand, increasing the amount of analysis that is done on the distributed monitors will obviously hinder the performance of the individual hosts." (12) [SYM_P_0069291] "The director is responsible for analyzing the events reported by the host and LAN monitors, and therefore will have access to the distributed audit data gathered by the various monitors. The director may then use these records in support of a directed	make the connection from a university computer system, and then repeatedly tried to gain access to several different computers at the external site. In cases like these, the intruder tries only a few logins on each machine (usually with different account names), which means that an IDS on each host may not flag the attack. Even if the behavior is recognized as an attack on the individual host, current IDS's are generally unable to correlate reports from multiple hosts; thus they cannot recognize the *doorknob* attack as such. Because DIDS aggregates and correlates data from multiple hosts and the network, it is in a position to recognize the doorknob attack by detecting the pattern of repeated failed logins even though there may be too few on a single host to alert that host's monitor. In another incident, our NSM recently observed an intruder gaining access to a computer using a guest account which did not require a password. Once the attacker had access to the system, he exhibited behavior which would have alerted most existing IDS's (e.g., changing passwords and failed events). In an incident such as this, DIDS would not only report the attack, but may also be able to identify the source of the attack. That is, while most IDS's would report the occurrence of an incident involving user "guest" on the target machine, DIDS would also report that user "guest" was really, for example, user "smith" on the source machine, assuming that the source machine was in the monitored domain. It may also be possible to go even further back and identify all of the

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
		investigation of a particular subject. The director communicates bidirectionally with the host and LAN monitors to facilitate the transfer of data and the processing of queries and responses. It is also able to correlate information obtained from the individual host and LAN monitors. The director also supports the user interface." (12) [SYM_P_0069291] "This paper presented an architecture for a Distributed Intrusion Detection System (DIDS). The target environment for DIDS is a heterogeneous network of computers that may consist of different hosts, servers, etc. The DIDS architecture consists of a collection of host monitors, each of which monitors a single host Computer; one or more LAN monitors, each of which monitors traffic on its corresponding LAN segment; and the DIDS director, which receives reports from the various monitors, correlates the data, and makes inferences regarding the security state of the system." (15) [SYM_P_0069294]	different user accounts in the "chain" to find the initial launching point of the attack. Another possible scenario is what we call *network browsing*. This occurs when a (network) user is looking through a number of files on several different computers within a short period of time. The browsing activity level on any single host may not be sufficiently high enough to raise any alarm by itself. However, the network-wide, aggregated browsing activity level may be high enough to raise suspicion on this user. Network browsing can be detected as follows. Each host monitor will report that a particular user is browsing on that system, even if the corresponding degree of browsing is small. The expert system can then aggregate such information from multiple hosts to determine that all of the browsing activity corresponds to the same network user. This scenario presents a key challenge for DIDS: the tradeoff between sending all audit records to the director versus missing attacks because thresholds on each host are not exceeded. In addition to the specific scenarios outlined above, there are a number of general ways that an intruder can use the connectivity of the network to hide his trail and to enhance his effectiveness. Some of the attack configurations which have been hypothesized include *chain* and *parallel* attacks [2]. DIDS combats these inherent vulnerabilities of the network by using the very same

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
			connectivity to help track and detect the intruder. Note that DIDS should be at least as effective as host-based IDS's (if we implement all of their functionality in the DIDS host monitor), and at least as effective as the stand-alone NSM." (168-69) [SYM_P_0077176- SYM_P_0077177] "The DIDS architecture combines distributed monitoring and data reduction with centralized data analysis." (169) [SYM_P_0077177] "Reports are sent independently and asynchronously from the host and LAN monitors to the DIDS director through a communications infrastructure (Fig. 2). High level communication protocols between the components are based on the ISO Common Management Information Protocol (CMIP) recommendations, allowing for future inclusion of CMIP management tools as they become useful. The architecture also provides for bidirectional communication between the DIDS director and any monitor in the configuration. This communication consists primarily of notable events and anomaly reports from the monitors. The director can also make requests for more detailed information from the distributed monitors via a 'GET' directive, and issue commands to have the distributed monitors modify their monitoring capabilities via a 'SET' directive." (169) [SYM_P_0077177] "The expert system is responsible for evaluating and reporting on

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
			the security state of the monitored system. It receives the reports from the host and the LAN monitors, and, based on these reports, it makes inferences about the security of each individual host, as well as the system as a whole." (169) [SYM_P_0077177] "Correlating data from several independent sources, including the network itself, can aid in recognizing this type of behavior and tracking an intruder to their source." (170) [SYM_P_0077178] "The expert system uses rules derived from the hierarchical Intrusion Detection Model (IDM). The IDM describes the data abstractions used in inferring an attack on a network of computers. That is, it describes the transformation from the distributed raw audit data to high level hypotheses about intrusions and about the overall security of the monitored environment. In abstracting and correlating data from the distributed sources, the model builds a virtual machine which consists of all the connected hosts as well as the network itself. This unified view of the distributed system simplifies the recognition of intrusive behavior which spans individual hosts. The model is also applicable to]he trivial network of a single computer." (172) [SYM_P_0077180] "Events in context are combined to create threats." (172) [SYM_P_0077180] "At the highest level, the model produces a numeric value

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
			between one and 100 which represents the overall *security state* of the network. The higher the number the less secure the network. This value is a function of all the threats for all the subjects on the system. Here again we treat the collection of hosts as a single distributed system. Although representing the security level of the system as a single value seems to imply some loss of information, it provides a quick reference point for the SSO. In fact, in the current implementation, no information is lost since the expert system maintains all the evidence used in calculating the security state in its internal database, and the SSO has access to that database." (173) [SYM_P_0077181] "The expert system shell consists of approximately a hundred lines of Prolog source code. The shell is responsible for reading new facts reported by the distributed monitors, attempting to apply the rules to the facts and hypotheses in the Prolog database, reporting suspected intrusions, and maintaining the various dynamic values associated with the rules and hypotheses." (173) [SYM_P_0077181] "In addition to the consideration of external temporal context, the expert system uses time windows to correlate events occurring in temporal proximity. This notion of temporal proximity implements the heuristic that a call to the UNIX *who* command followed closely by a *login* or *logout* is more likely to be related to an intrusion than either of those events occurring alone. Spatial

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
			context implies the relative importance of the source of events. That is, events related to a particular user, or events from a particular host, may be more likely to represent an intrusion than similar events from a different source. For instance, a user moving from a low-security machine to a high-security machine may be of greater concern than a user moving in the opposite direction. The model also allows for the correlation of multiple events from the same user or source. In both of these cases, the multiple events are more noteworthy when they have a common element than when they do not." (172) [SYM_P_0077180]
3	The method of claim 1, wherein integrating further comprises invoking countermeasures to a suspected attack.	"We anticipate that a growing set of tools will be used in conjunction with the intrusion detection functions of DIDS. Among these will include incident handling tools. Depending on the level of expertise of the SSO, these tools could include online explicit instructions, e.g., "who to call" lists, automatic response procedures, etc. In addition to the incident handling tools, the user interface can provide access to standard network administration tools; in particular, we are evaluating the SNMP tools currently available." (15) [SYM_P_0069294] "The proposed architecture for this distributed intrusion-detection system consists of the following components: a host manager (viz. a monitoring process or collection of processes running in background) in each host; a LAN manager for monitoring each	"We anticipate that a growing set of tools, including incident-handling tools and network-management tools, will be used in conjunction with the intrusion-detection functions of DIDS. This will give the SSO the ability to actively respond to attacks against the system in real-time. Incident-handling tools may consist of possible courses of action to take against an attacker, such as cutting off network access, a directed investigation of a particular user, removal of system access, etc. Network-management tools that are able to perform network mapping would also be useful." (169-70) [SYM_P_0077177- SYM_P_0077178] "The architecture also provides for bidirectional communication between the DIDS director and any monitor in the configuration. This communication consists primarily of notable events and

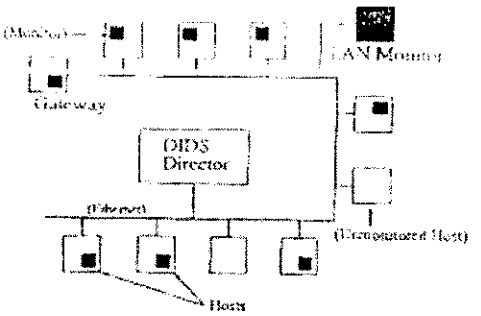
Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
		LAN in the system; and a central manager which is placed at a single secure location and which receives reports from various host and LAN managers to process these reports, correlate them, and detect intrusions." (1) [SYM_P_0069280] "The director's user interface serves both the intrusion detection and the incident management components of DIDS. It is designed to take advantage of the graphic capabilities of the target platform (a Sun SPARCstation 1). The user interface is hierarchical in its presentation of information, allowing the SSO to display as much, or as little, of the information available from DIDS as he/she wants. In its most compact form, the interface is reduced to a state meter displaying a measure of the security state of the network as evaluated by DIDS. Other options include a control panel for access to system management tools, displays of summary or detailed monitoring of the net, of hosts or of users, and a query capability for the distributed audit data. The user interface is designed to be extensible, so that new functionality can he added without undue effort." (15) [SYM_P_0069294]	anomaly reports from the monitors." (169) [SYM_P_0077177]
4	The method of claim 1, wherein the plurality of network monitors include an API for encapsulation of monitor functions and	"We anticipate that a growing set of tools will be used in conjunction with the intrusion detection functions of DIDS. Among these will include incident handling tools. Depending on the level of expertise of the SSO, these tools could include online explicit instructions, e.g., "who to call" lists, automatic response	"High level communication protocols between the components are based on the ISO Common Management Information Protocol (CMIP) recommendations, allowing for future inclusion of CMIP management tools as they become useful." (169) [SYM_P_0077177]

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	integration of third-party tools.	procedures, etc. In addition to the incident handling tools, the user interface can provide access to standard network administration tools; in particular, we are evaluating the SNMP tools currently available." (15) [SYM_P_0069294]	"We anticipate that a growing set of tools, including incident-handling tools and network-management tools, will be used in conjunction with the intrusion-detection functions of DIDS." (169) [SYM_P_0077177]
5	The method of claim 1, wherein the enterprise network is a TCP/IP network.	"On the other hand, standard network protocols exist (e.g., TCP/IP and UDP/IP) which most major operating systems support and use. By using these network standards, the NSM can monitor a heterogeneous set of hosts and operating systems simultaneously." (9) [SYM_P_0069288] "The next layer, called the *thread layer*, accepts as input the time-augmented packets from the packet layer. These packets are then correlated into unidirectional data streams. Each stream consists of the data (with the different layers of protocol headers removed) being transferred from one host to another host by a particular protocol (TCP/IP or UDP/IP), through a unique set (for the particular set of hosts and protocol) of ports. This stream of data, which is called a thread, is mapped into a *thread vector*. All the thread vectors are passed up to the third layer." (10) [SYM_P_0069289]	The LAN monitor is currently a subset of UC Davis' Network Security Monitor [3]. The LAN monitor builds its own "LAN audit trail". The LAN monitor observes each and every packet on its segment of the LAN and, from these packets, it is able to construct higher-level objects such as connections (logical circuits), and service requests using the TCP/IP or UDP/IP protocols. In particular, it audits host-to-host connections, services used, and volume of traffic per connection. (171) [SYM_P_0077179]
6	The method of claim 1, wherein the network	"The generalized distributed environment is heterogeneous, i.e., the network nodes can be hosts or servers from different vendors,	"In addition to the current host monitor, which is designed to detect attacks on general purpose multi-user computers, we intend

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}.	or some of them could be LAN managers, like our previous work, a network security monitor (NSM), as well." (1) [SYM_P_0069280] **103:** NetRanger: NetRanger User's Guide 1.3.1, WheelGroup Corporation, 1997 [SYM_P_0074948-82], 1-6 [SYM_P_0074979], 2-3 to 2-4 [SYM_P_0074996-97]	to develop monitors for application specific hosts such as file servers and gateways. In support of the ongoing development of DIDS we are planning to extend our model to a hierarchical Wide Area Network environment." (174) [SYM_P_0077182]  Fig. 1. DIDS Target Environment [SYM_P_0077184]
7	The method of claim 1, wherein deploying the network monitors includes	"The proposed architecture for this distributed intrusion-detection system consists of the following components: a host manager (viz. a monitoring process or collection of processes running in	"In support of the ongoing development of DIDS we are planning to extend our model to a hierarchical Wide Area Network environment." (174) [SYM_P_0077182]

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	placing a plurality of service monitors among multiple domains of the enterprise network.	background) in each host; a LAN manager for monitoring each LAN in the system; and a central manager which is placed at a single secure location and which receives reports from various host and LAN managers to process these reports, correlate them, and detect intrusions." (1) [SYM_P_0069280] "In DIDS, the monitoring and analysis functions are distributed among several components. These components include a *DIDS director*, a collection of host monitors, and at least one *LAN monitor*. The host and LAN monitors are primarily responsible for detecting single events and known attack signatures which have a high probability of being relevant to the security of a system; so they must constantly monitor their respective domains." (12) [SYM_P_0069291]	"The DIDS components include the DIDS director, a single host monitor per host, and a single LAN monitor for each LAN segment of the monitored network." (168) [SYM_P_0077176] "In another incident, our NSM recently observed an intruder gaining access to a computer using a guest account which did not require a password. Once the attacker had access to the system, he exhibited behavior which would have alerted most existing IDS's (e.g., changing passwords and failed events). In an incident such as this, DIDS would not only report the attack, but may also be able to identify the source of the attack. That is, while most IDS's would report the occurrence of an incident involving user "guest" on the target machine, DIDS would also report that user "guest" was really, for example, user "smith" on the source machine, assuming that the source machine was in the monitored domain. It may also be possible to go even further back and identify all of the different user accounts in the "chain" to find the initial launching point of the attack." (168) [SYM_P_0077176]
8	The method of claim 7, wherein receiving and integrating is performed by a domain monitor with respect to a plurality of service monitors within the	"The proposed architecture for this distributed intrusion-detection system consists of the following components: a host manager (viz. a monitoring process or collection of processes running in background) in each host; a LAN manager for monitoring each LAN in the system; and a central manager which is placed at a single secure location and which receives reports from various	"In support of the ongoing development of DIDS we are planning to extend our model to a hierarchical Wide Area Network environment." (174) [SYM_P_0077182] "The DIDS components include the DIDS director, a single host monitor per host, and a single LAN monitor for each LAN segment of the monitored network." (168) [SYM_P_0077176]

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	domain monitor's associated network domain.	host and LAN managers to process these reports, correlate them, and detect intrusions." (1) [SYM_P_0069280] "In DIDS, the monitoring and analysis functions are distributed among several components. These components include a *DIDS director*, a collection of host monitors, and at least one *LAN monitor*. The host and LAN monitors are primarily responsible for detecting single events and known attack signatures which have a high probability of being relevant to the security of a system; so they must constantly monitor their respective domains." (12) [SYM_P_0069291]	"In another incident, our NSM recently observed an intruder gaining access to a computer using a guest account which did not require a password. Once the attacker had access to the system, he exhibited behavior which would have alerted most existing IDS's (e.g., changing passwords and failed events). In an incident such as this, DIDS would not only report the attack, but may also be able to identify the source of the attack. That is, while most IDS's would report the occurrence of an incident involving user "guest" on the target machine, DIDS would also report that user "guest" was really, for example, user "smith" on the source machine, assuming that the source machine was in the monitored domain. It may also be possible to go even further back and identify all of the different user accounts in the "chain" to find the initial launching point of the attack." (168) [SYM_P_0077176]
9	The method of claim 1, wherein deploying the network monitors includes deploying a plurality of domain monitors within the enterprise network, each domain monitor being associated with a corresponding domain of	See '203 claim 8 **103:** NetRanger. *See* NetRanger User's Guide 1.3.1, WheelGroup Corporation, 1997 [SYM_P_0074948-5282]. ISM. *See* L.T. Heberlein et al., "Internetwork Security Monitor," Proc. of the 15th National Computer Security Conference,	See '203 claim 8 **103:** NetRanger. *See* NetRanger User's Guide 1.3.1, WheelGroup Corporation, 1997 [SYM_P_0074948-5282]. ISM. *See* L.T. Heberlein et al., "Internetwork Security Monitor," Proc. of the 15th National Computer Security Conference,

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	the enterprise network.	October 1992, 262-271 [SYM_P_0069244-54]. GrIDS. *See* S.S. Chen et al, "GrIDS – A graph based intrusion detection system for large networks," 19th National Information Systems Security Conference (1996) [SYM_P_0068883 – SYM_P_0068892]. P. Porras and P. Neumann, "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances", 20th NISSC October 9, 1997 [SYM_P_0068831- SYM_P_0068843].	October 1992, 262-271 [SYM_P_0069244-54]. GrIDS. *See* S.S. Chen et al, "GrIDS – A graph based intrusion detection system for large networks," 19th National Information Systems Security Conference (1996) [SYM_P_0068883 – SYM_P_0068892]. P. Porras and P. Neumann, "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances", 20th NISSC October 9, 1997 [SYM_P_0068831- SYM_P_0068843].
10	The method of claim 9, wherein receiving and integrating is performed by an enterprise monitor with respect to a plurality of domain monitors within the enterprise network.	See '203 claim 8 "The proposed architecture for this distributed intrusion-detection system consists of the following components: a host manager (viz. a monitoring process or collection of processes running in background) in each host; a LAN manager for monitoring each LAN in the system; and a central manager which is placed at a single secure location and which receives reports from various host and LAN managers to process these reports, correlate them, and detect intrusions." (1) [SYM_P_0069280] **103:**	See '203 claim 8 "The DIDS components include the DIDS director, a single host monitor per host, and a single LAN monitor for each LAN segment of the monitored network. The information gathered by these distributed components is transported to, and analyzed at, a central location (viz. an expert system, which is a sub-component of the director), thus providing the capability to aggregate information from different sources." (168) [SYM_P_0077176] "The architecture also provides for bidirectional communication between the DIDS director and any monitor in the configuration. This communication consists primarily of notable events and

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
		NetRanger. *See* NetRanger User's Guide 1.3.1, WheelGroup Corporation, 1997 [SYM_P_0074948-5282]. ISM. *See* L.T. Heberlein et al., "Internetwork Security Monitor," Proc. of the 15th National Computer Security Conference, October 1992, 262-271 [SYM_P_0069244-54]. GrIDS. *See* S.S. Chen et al, "GrIDS – A graph based intrusion detection system for large networks," 19th National Information Systems Security Conference (1996) [SYM_P_0068883 – SYM_P_0068892]. P. Porras and P. Neumann, "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances", 20th NISSC October 9, 1997 [SYM_P_0068831- SYM_P_0068843].	anomaly reports from the monitors." (169) [SYM_P_0077177] **103:** NetRanger. *See* NetRanger User's Guide 1.3.1, WheelGroup Corporation, 1997 [SYM_P_0074948-5282]. ISM. *See* L.T. Heberlein et al., "Internetwork Security Monitor," Proc. of the 15th National Computer Security Conference, October 1992, 262-271 [SYM_P_0069244-54]. GrIDS. *See* S.S. Chen et al, "GrIDS – A graph based intrusion detection system for large networks," 19th National Information Systems Security Conference (1996) [SYM_P_0068883 – SYM_P_0068892]. P. Porras and P. Neumann, "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances", 20th NISSC October 9, 1997 [SYM_P_0068831- SYM_P_0068843].
11	The method of claim 9, wherein the plurality of domain monitors within the enterprise network establish	**103:** CSM. *See* Maj. Gregory B. White et al., "Cooperating Security Manager – A Peer-Based Intrusion Detection Approach," IEEE	**103:** CSM. *See* Maj. Gregory B. White et al., "Cooperating Security Manager – A Peer-Based Intrusion Detection Approach," IEEE

Distributed Intrusion Detection System
"DIDS February 1991 and DIDS October 1991"

'203 Claim number	Claim Term	DIDS February 1991 (printed publication and public use)	DIDS October 1991 (printed publication and public use)
	peer-to-peer relationships with one another.	Network (January/February 1996) [SYM_P_0069980-83] ISM: L.T. Heberlein et al., "Internetwork Security Monitor," Proc. of the 15th National Computer Security Conference, October 1992, pp. 262-271 [SYM_P_0069244-54], 268-70 [SYM_P_0069250-52] Network Security Probe. *See* P. Rolin, L. Toutain, and S. Gombault, "Network Security Probe," Proc. of the 2nd ACM Conference on Computer and Communications Security, 229-40 (ACM 1994) [SYM_P_0074513-24].	Network (January/February 1996) [SYM_P_0069980-83] ISM: L.T. Heberlein et al., "Internetwork Security Monitor," Proc. of the 15th National Computer Security Conference, October 1992, pp. 262-271 [SYM_P_0069244-54], 268-70 [SYM_P_0069250-52] Network Security Probe. *See* P. Rolin, L. Toutain, and S. Gombault, "Network Security Probe," Proc. of the 2nd ACM Conference on Computer and Communications Security, 229-40 (ACM 1994) [SYM_P_0074513-24].
12	An enterprise network monitoring system comprising:	See '203 claim 1	See '203 claim 1
	a plurality of network monitors deployed within an enterprise network;	See '203 claim 1	See '203 claim 1
	said plurality of network monitors detecting suspicious network activity	See '203 claim 1	See '203 claim 1
	based on analysis of network traffic data selected from the following categories: {network packet	See '203 claim 1	See '203 claim 1